U.S. Department of Justice

United States Attorney
District of New Jersey

970 Broad Street, 7th floor
Newark, New Jersey 07102

973-645-2700

June 17, 2019

Hon. Madeline Cox Arleo
United States District Judge
District of New Jersey
Martin Luther King Building & U.S. Courthouse
50 Walnut Street
Newark, NJ 07101

Re: United States v. Richard Adebayo
Criminal No. 19-68 (MCA)

Dear Judge Arleo:

The United States respectfully submits this letter brief to address the Defendant Richard Adebayo's Motion to Suppress the Apple laptop ("the Laptop") computer and evidence derived therefrom. Following the defendant's arrest on April 1, 2014, no member of law enforcement accessed or searched the Laptop prior to obtaining a search warrant for the Laptop on April 11, 2014. Accordingly, no Fourth Amendment violation occurred and the Defendant's motion is meritless.

On April 1, 2014, at approximately 7:45pm, the Millburn Police Department arrested the Defendant at the Short Hills Mall. A search incident to arrest revealed the Defendant was in possession of the Laptop at the time of his apprehension. The arresting officer who retrieved the Laptop from the Defendant did not attempt to determine if the Laptop was powered on. Following the arrest, the Defendant and the Laptop were transferred to the Millburn Police Department. On April 1, 2014, the Laptop was entered into evidence by the Millburn Police Department. On April 2, 2014, at approximately 2:30pm, HSI Special Agent Ricky Miller ("SA Miller") took custody of the Laptop and observed the device was powered on. HSI computer forensic practices discourage agents and forensic analysts from powering down seized electronic devices that are

found powered on.[1] Accordingly, SA Miller left the Laptop powered on and secured it in HSI custody until the Laptop was lawfully searched pursuant to a search warrant that was secured on April 11, 2014. After a search warrant for the Laptop was secured on April 11, 2014, HSI Special Agent William Belanger began his forensic analysis, determined the Laptop was powered on, and performed a soft shut down of the Laptop. The Laptop was then forensically imaged.

In the instant motion, the Defendant asserts that "operating system activity" occurred on the Laptop prior to the Government obtaining a search warrant for the Laptop. Specifically, the Defendant alleges that files on the Laptop were accessed, modified, and created. The Defendant concedes in the motion there is no evidence the pre-warrant operating system activity was "knowing and intentional." (ECF 43 at 3). Moreover, the Defendant's own expert further concedes "there is no way to determine who did what on the device" and what caused the operating system activity prior to the execution of the search warrant. (Defendant's Forensic Technician Report at page 2).

Despite these glaring concessions that fail to identify any unconstitutional action by law enforcement, the Defendant alleges law enforcement violated the Fourth Amendment. The Defendant's claims are unfounded. Law enforcement did not search the Laptop before the search warrant was obtained. The forensic image of the Laptop reveals the device remained powered on after it was lawfully seized on April 1, 2014. The operating system activity on the Laptop that occurred following the Defendant's arrest is likely attributable to activities that automatically occur while the Laptop was in a "power nap" mode.[2] According to Apple Inc., operating system and certain software application activity that can occur while the Laptop was in "power nap" mode includes:

- Mail receives new messages.
- Contacts keep up to date with changes made on other devices.
- Calendar receives new invitations and calendar updates.
- Reminders keep up to date with changes made on other devices.
- Notes keep up to date with changes made on other devices.

---

[1] Best practices for preserving data on a powered-on electronic device discourages analysts from powering down the device because of the potential loss of random access memory that may contain data related to the device's passwords and other potential data that may have investigatory value. Additionally, powering down a powered-on device could encrypt the data on the device and prevent law enforcement from securing potentially relevant data contained on the device.

[2] According to Apple Inc., the Defendant's Laptop was equipped with a "power nap" feature that allowed operating system activity to occur while the device is "asleep". *See* https://support.apple.com/en-us/HT204032

- Documents stored in iCloud keep up to date with changes made on other devices.
- Photo Stream keeps up to date with changes made on other devices.
- Find My Mac updates the location of the Mac, so you can find it while it's asleep.
- VPN on demand continues working so that your corporate email updates securely. (Power Nap supports VPN connections that use a certificate to authenticate, not VPN connections that require entering a password.)
- Mobile Device Management can remotely lock and wipe your Mac.[3]

The operating system activity the Defendant argues occurred before the search warrant was obtained appears to be internet based activity that the Laptop was designed to do when in its "power nap" mode. None of the operating system activity that occurred on the device prior to April 11, 2014 is attributable to law enforcement. Accordingly, the Defendant's motion must be denied. The Defendant's additional assertion that "proper forensic procedures were not followed" is also meritless. Moreover, such an assertion relates to weight and not admissibility.

For the foregoing reasons, the Defendant's Motion to Suppress Evidence (ECF No. 43) should be denied.

Respectfully submitted,

CRAIG CARPENITO
United States Attorney

/s/ Catherine R. Murphy
By: JAMEL SEMPER
CATHERINE R. MURPHY
Assistant U.S. Attorneys

[3] *Id.*